

FIG.1

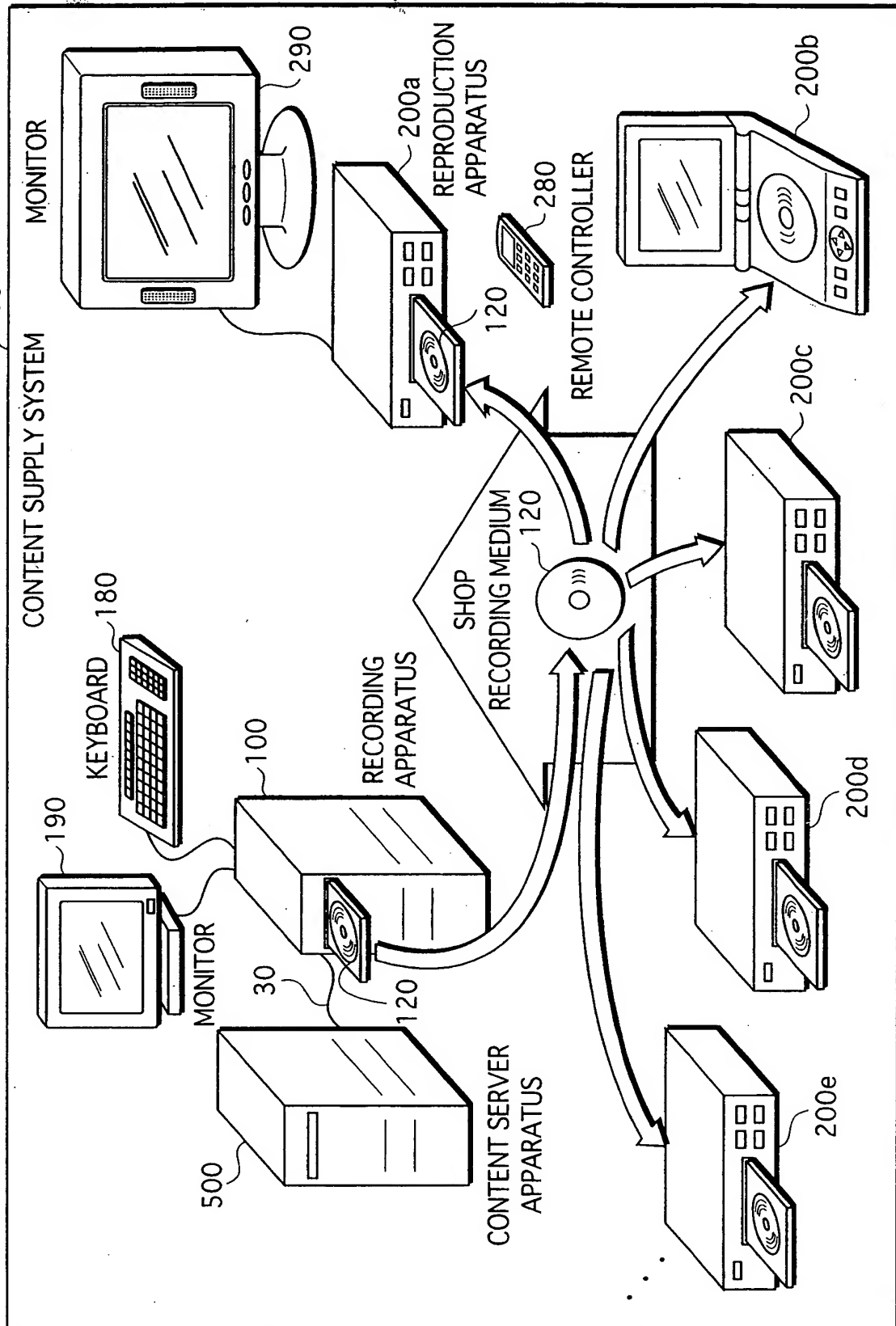


FIG.2

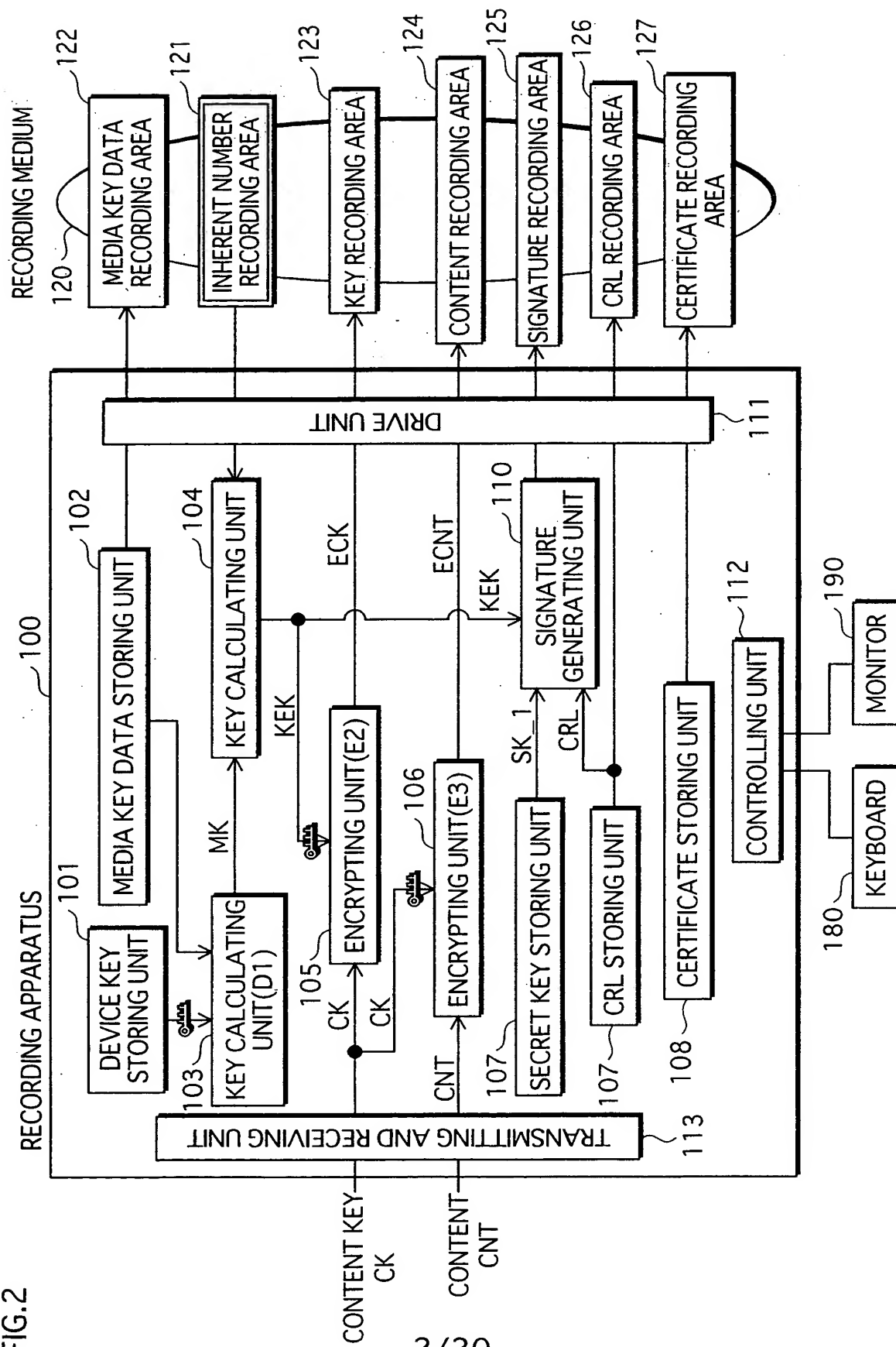


FIG.3

RECORDING MEDIUM

120

INHERENT NUMBER RECORDING AREA

MEDIUM INHERENT NUMBER
MID(0x000000006)

121

122

MEDIA KEY DATA RECORDING AREA

MEDIA KEY DATA MDATA	
ENCRYPTED MEDIA KEY E1(DK_1, MK)	APPARATUS NUMBER (1)
ENCRYPTED MEDIA KEY E1(DK_2, MK)	APPARATUS NUMBER (2)
ENCRYPTED MEDIA KEY E1(DK_3, 0)	APPARATUS NUMBER (3)
ENCRYPTED MEDIA KEY E1(DK_4, 0)	APPARATUS NUMBER (4)
ENCRYPTED MEDIA KEY E1(DK_5, MK)	APPARATUS NUMBER (5)
⋮	⋮
ENCRYPTED MEDIA KEY E1(DK_n-1, MK)	APPARATUS NUMBER (n-1)
ENCRYPTED MEDIA KEY E1(DK_n, MK)	APPARATUS NUMBER (n)

123

KEY RECORDING AREA

ENCRYPTED CONTENT KEY
ECK(E2(KEK, CK))

124

CONTENT RECORDING AREA

ENCRYPTED CONTENT
ECNT(E3(CK, CNT))

125

SIGNATURE RECORDING AREA

SIGNATURE DATA
SigCRL(Sig(SK_1, KEK || CRL))

126

CRL RECORDING AREA

606

REVOCATION LIST CRL	
ID_3 (0x000000003)	
ID_4 (0x000000004)	
SigID(Sig(SK_CA, ID_3 ID_4))	
VERSION NUMBER	

129

127

CERTIFICATE RECORDING AREA

607

PUBLIC KEY CERTIFICATE PKC	
ID_1 (0x000000001)	
PK_1	
Sig(SK_CA, ID_1 PK_1)	

FIG. 4

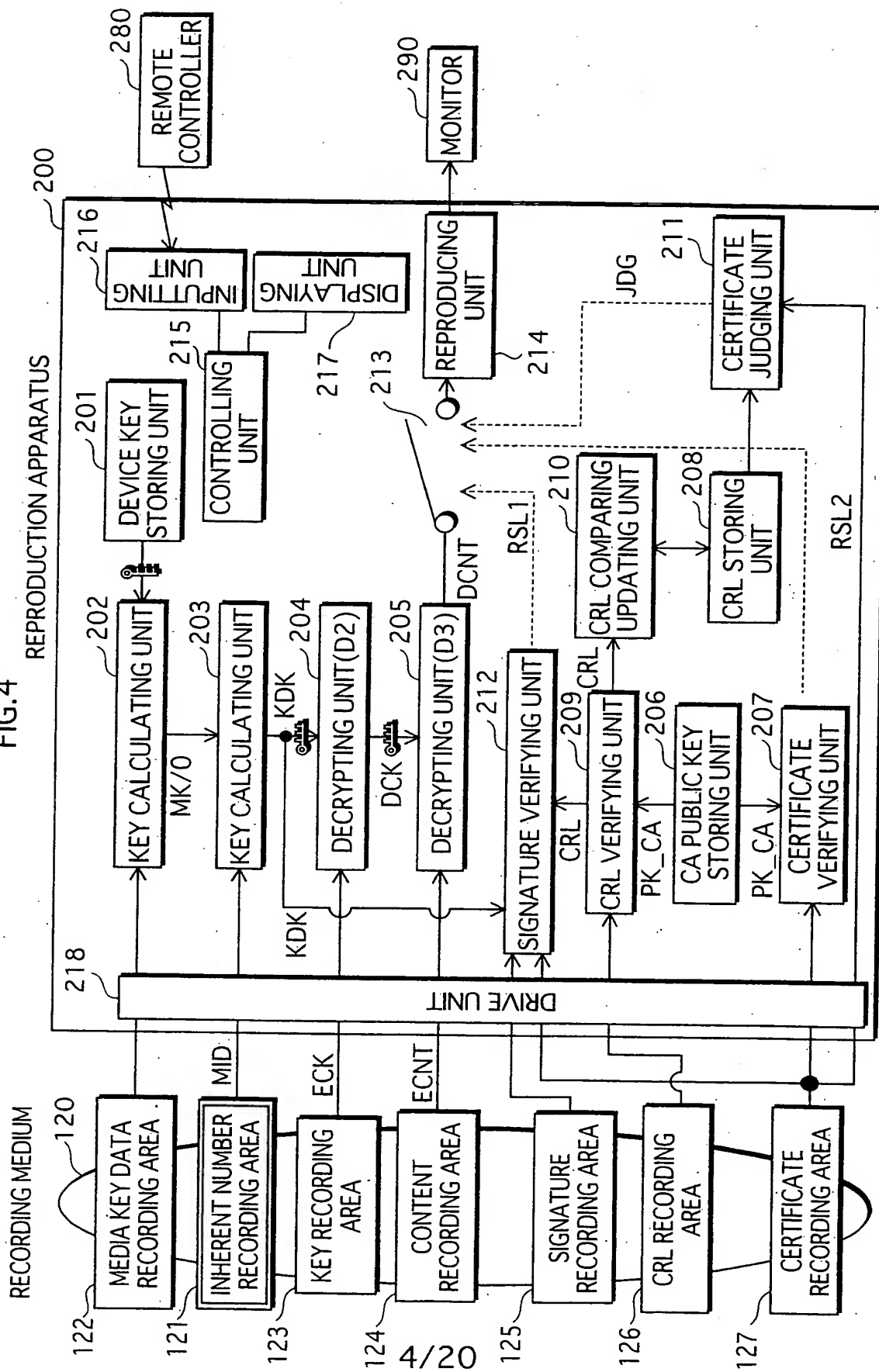


FIG. 5

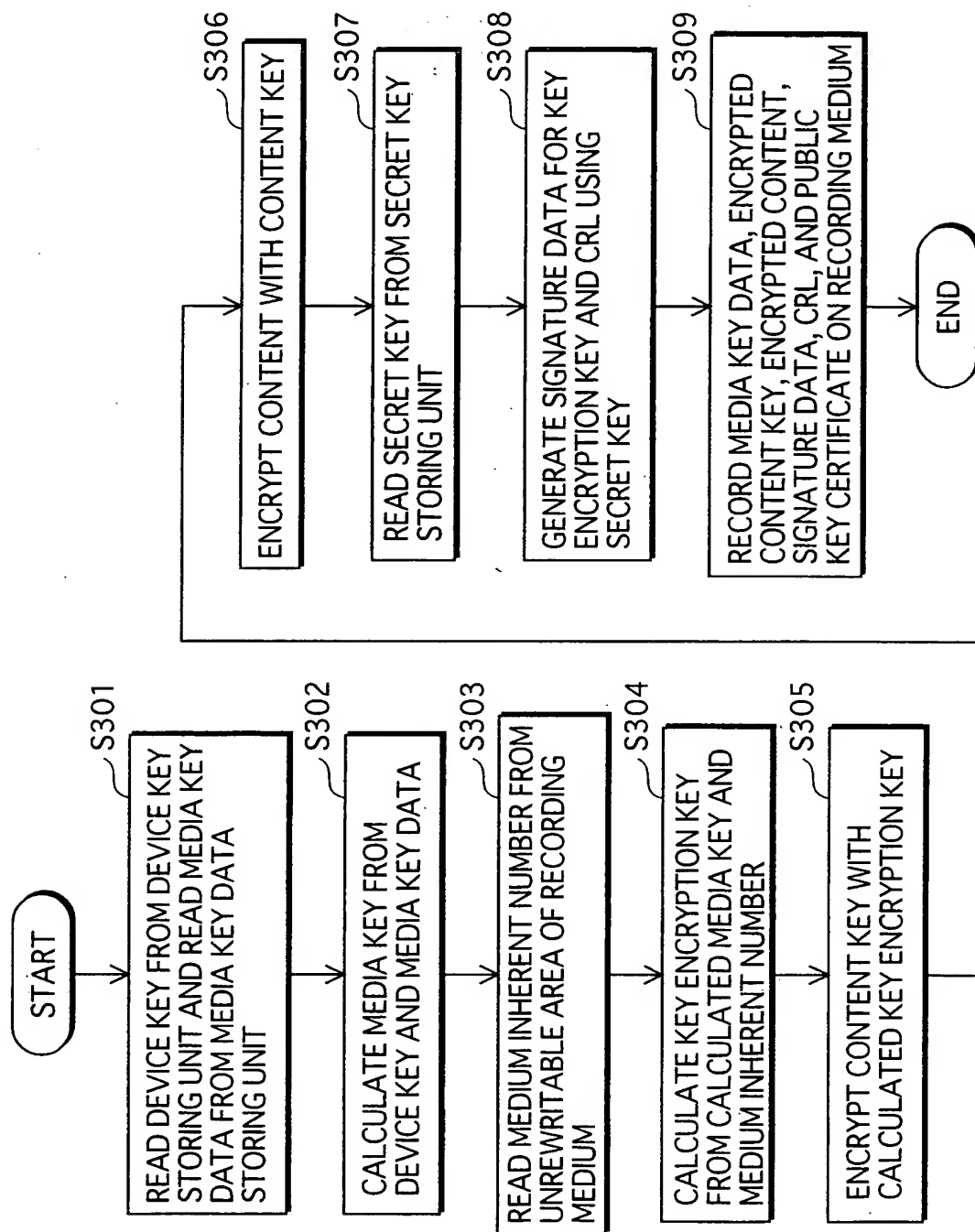


FIG.6

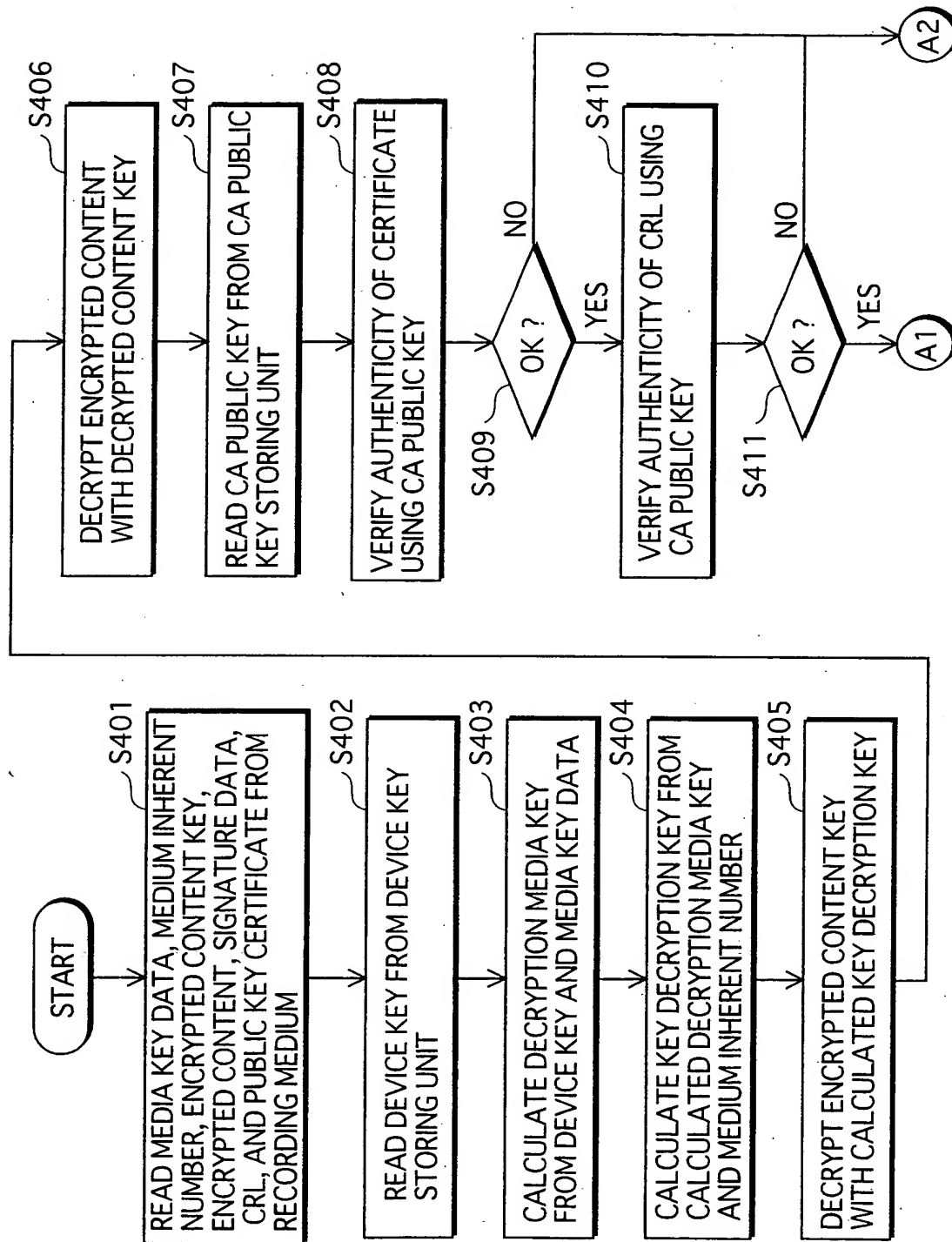


FIG. 7

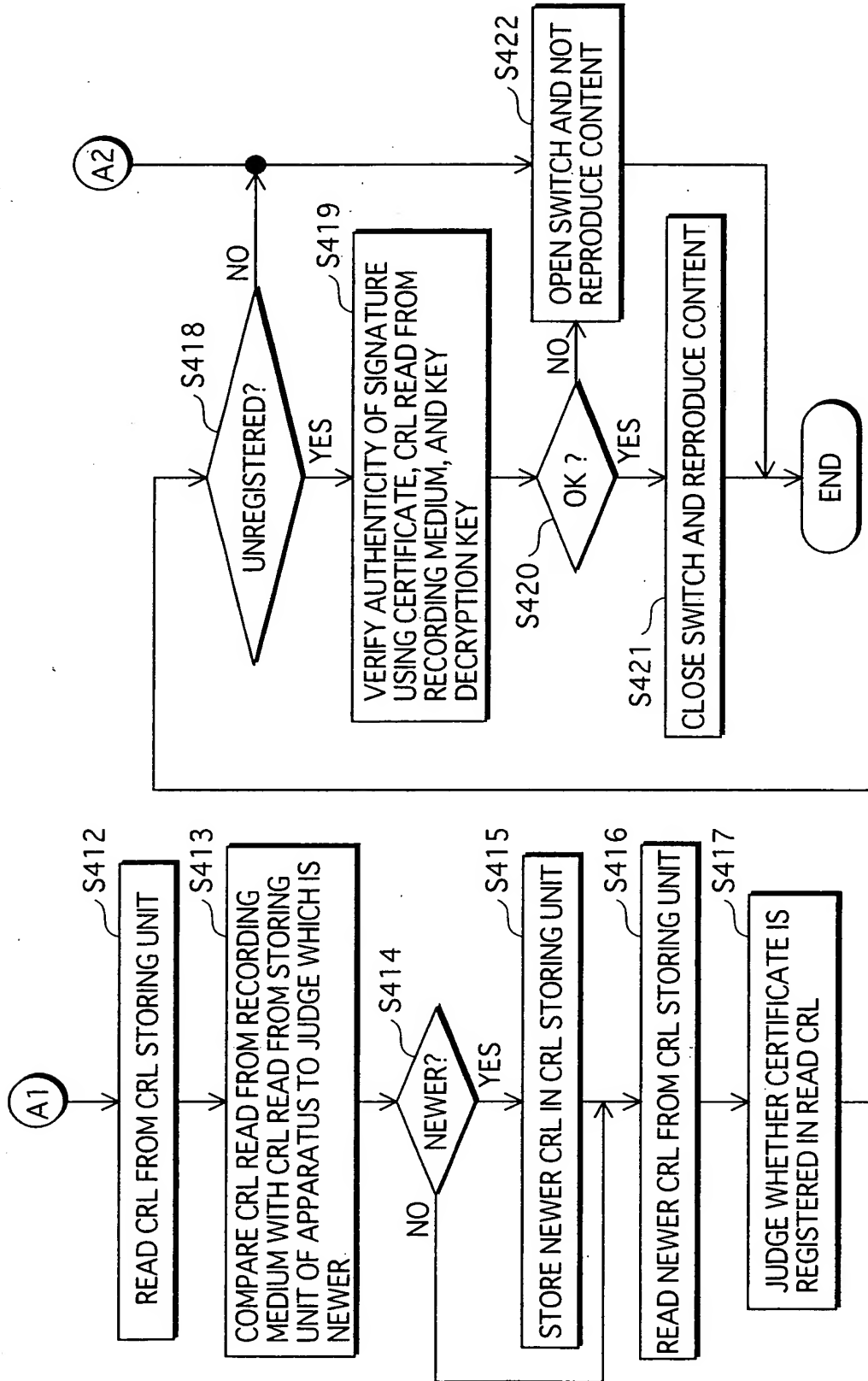


FIG.8

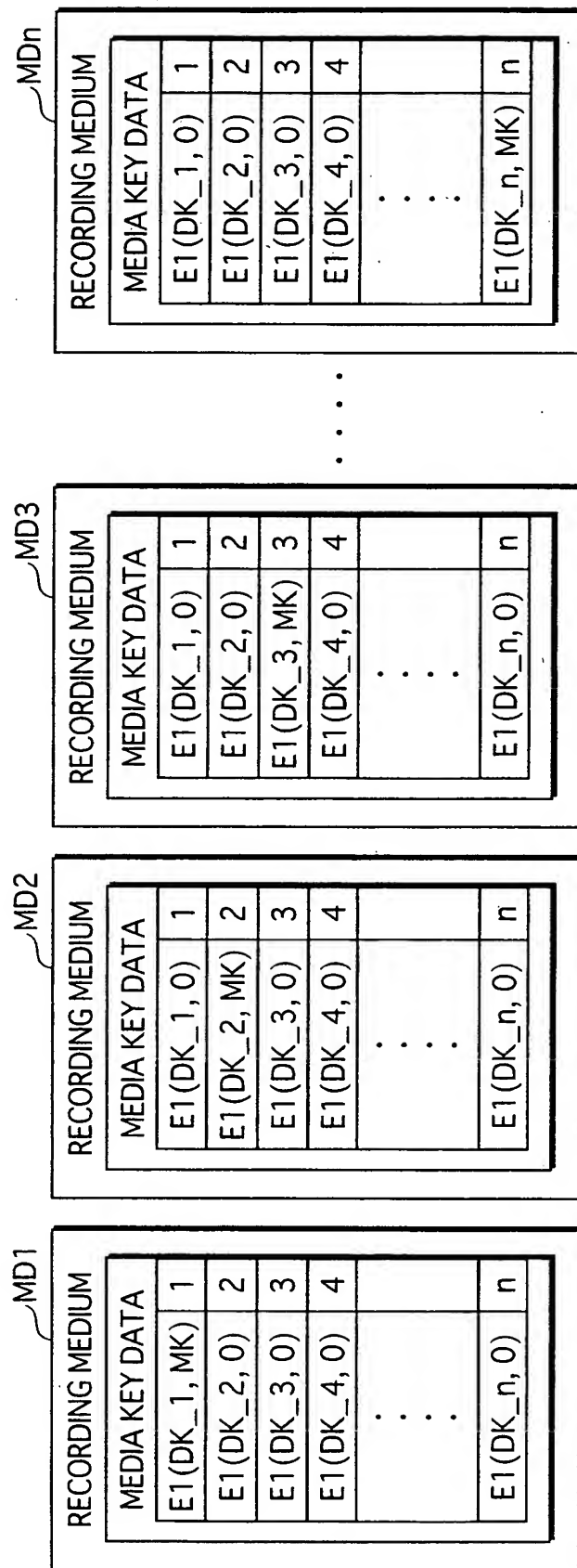


FIG.9

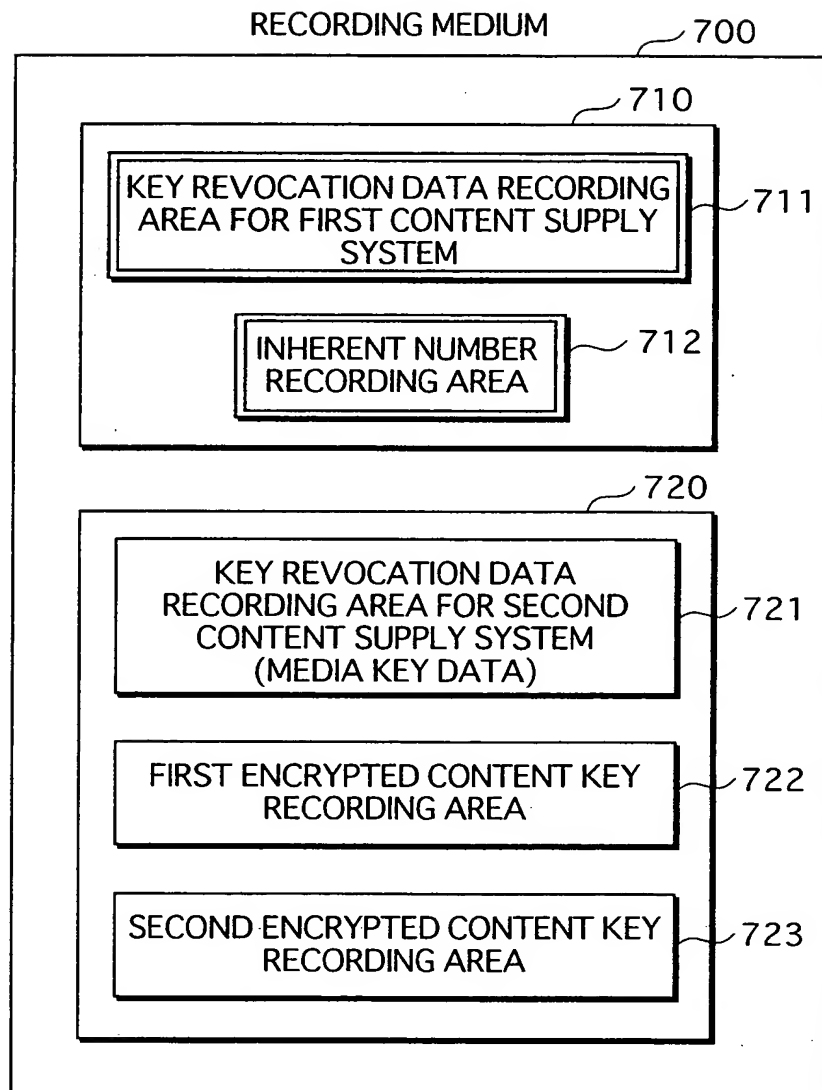


FIG.10

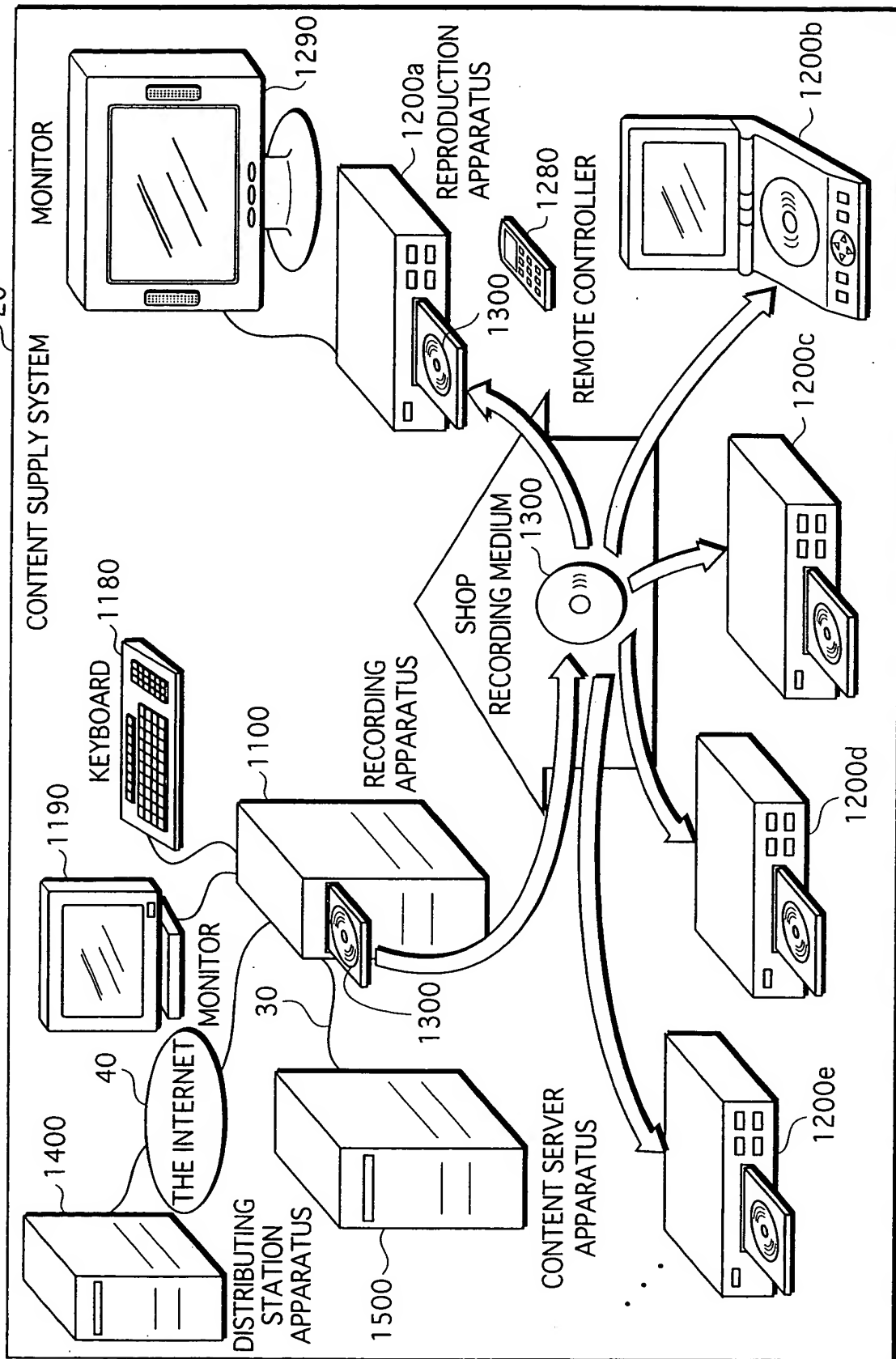


FIG. 11

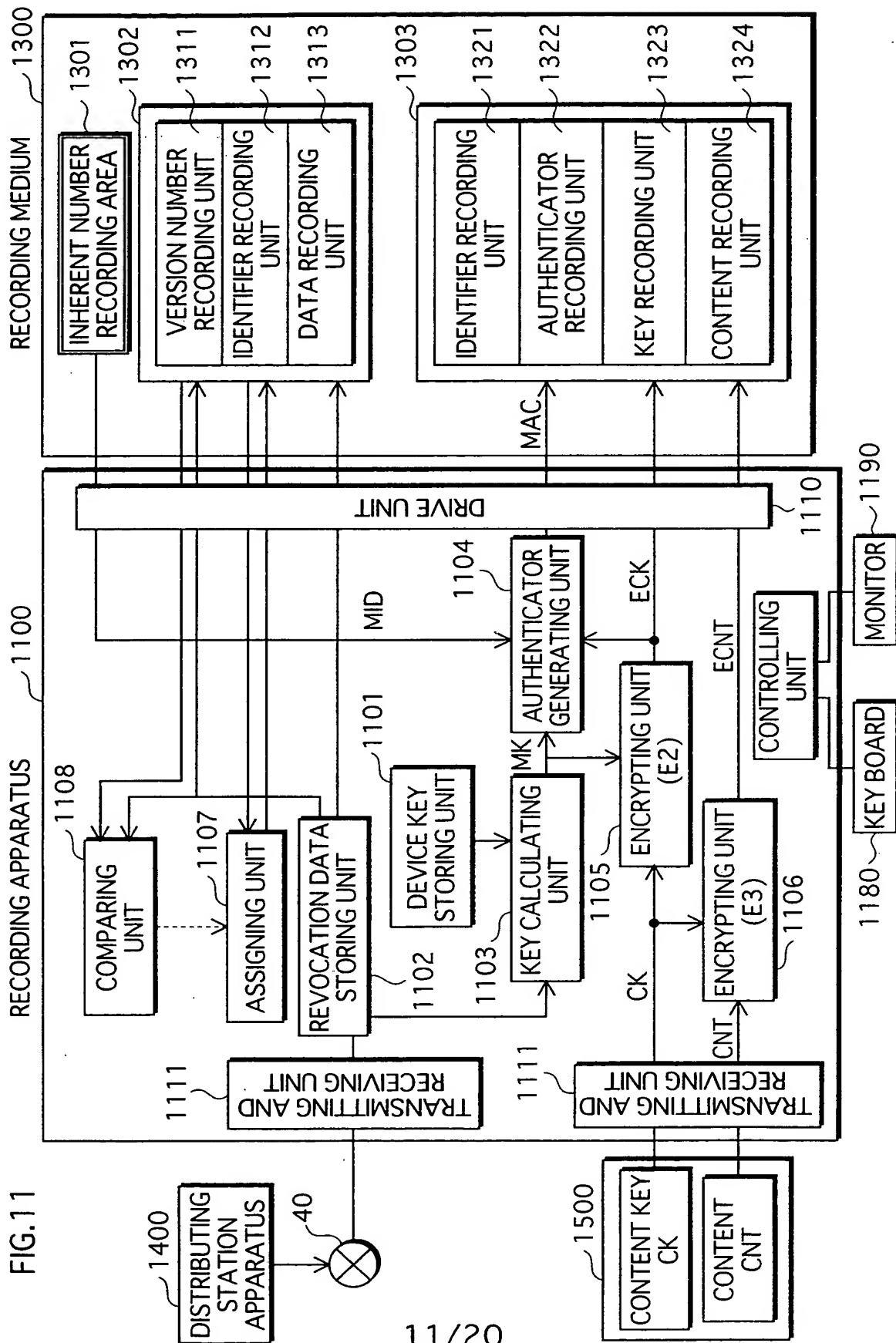


FIG.12

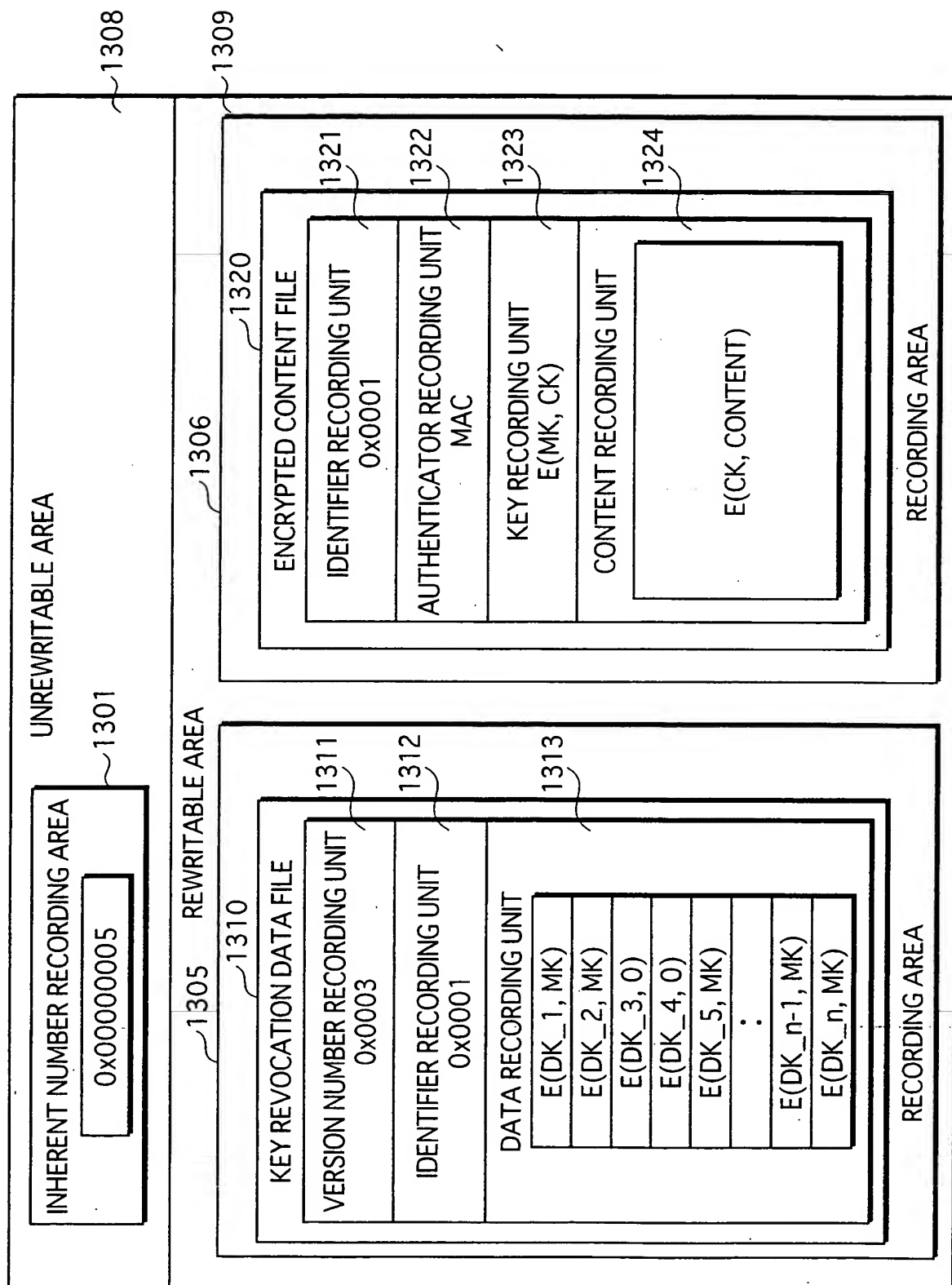


FIG.13

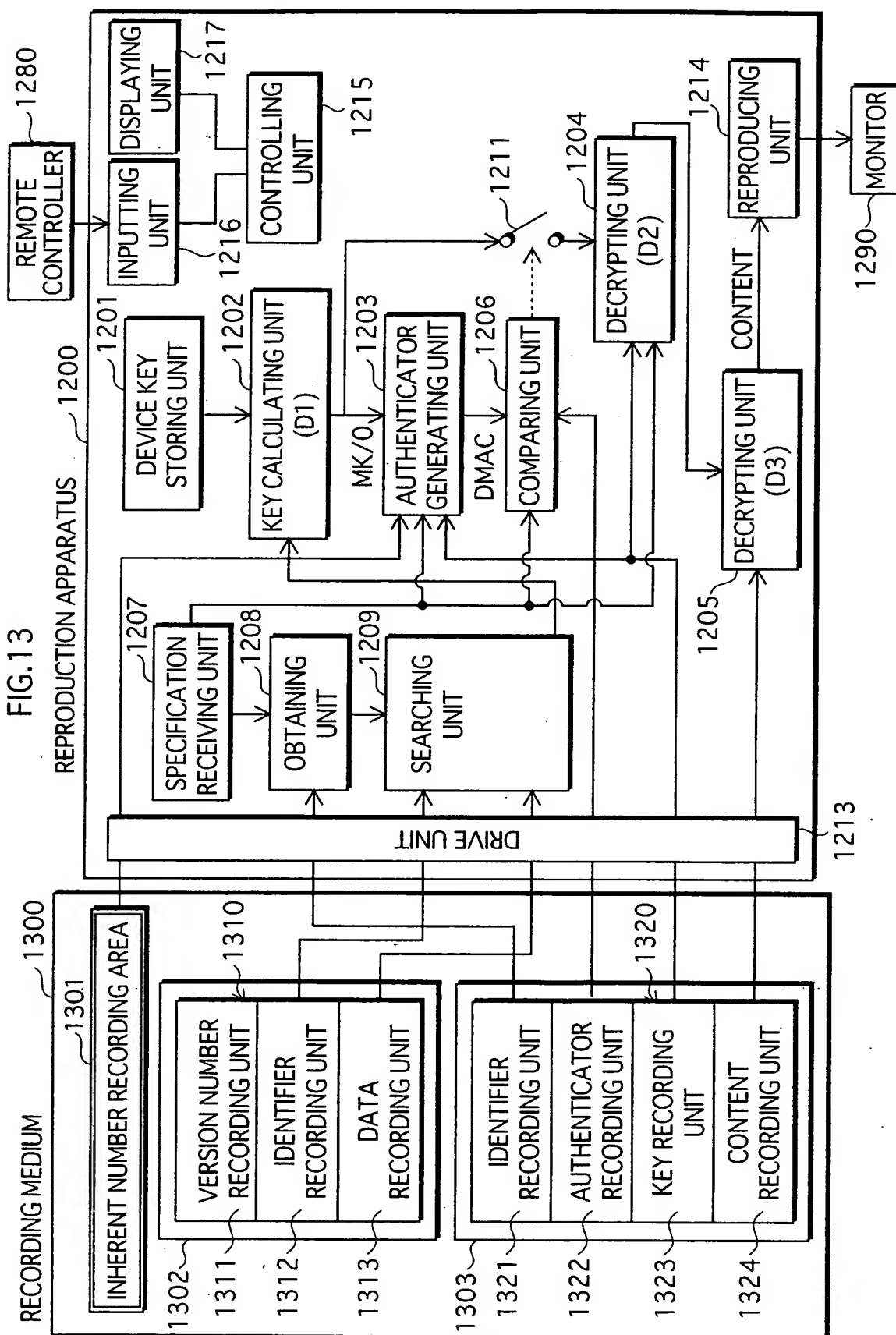


FIG.14

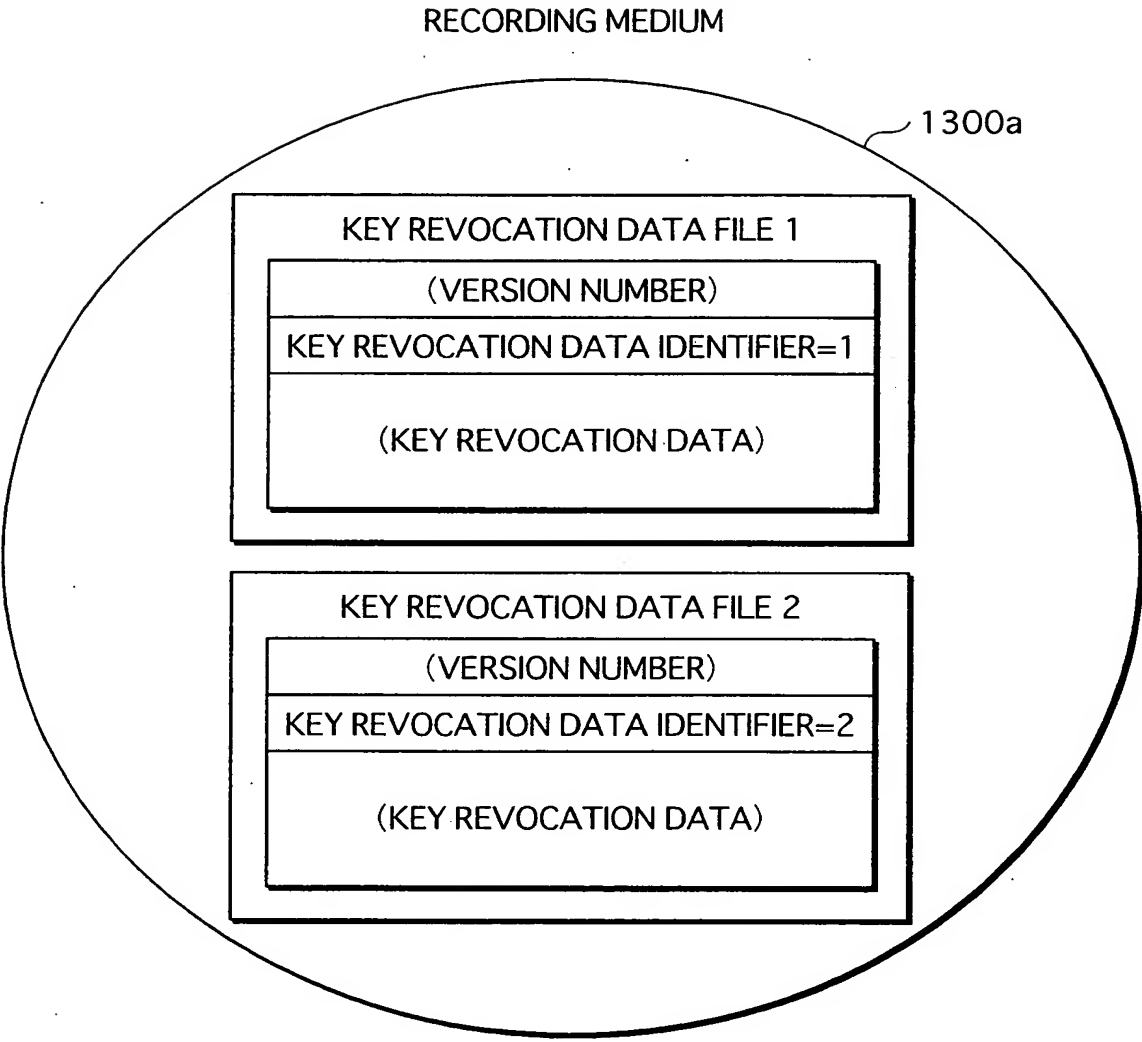


FIG. 15

RECORDING MEDIUM

1300b

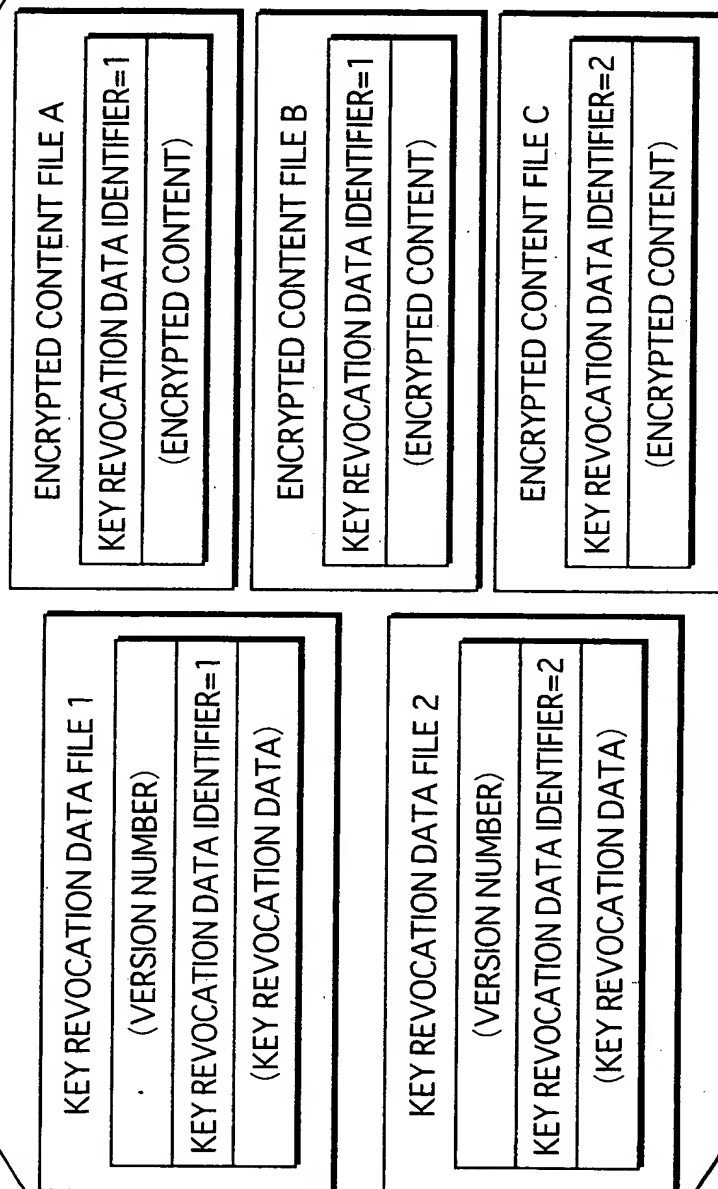


FIG.16

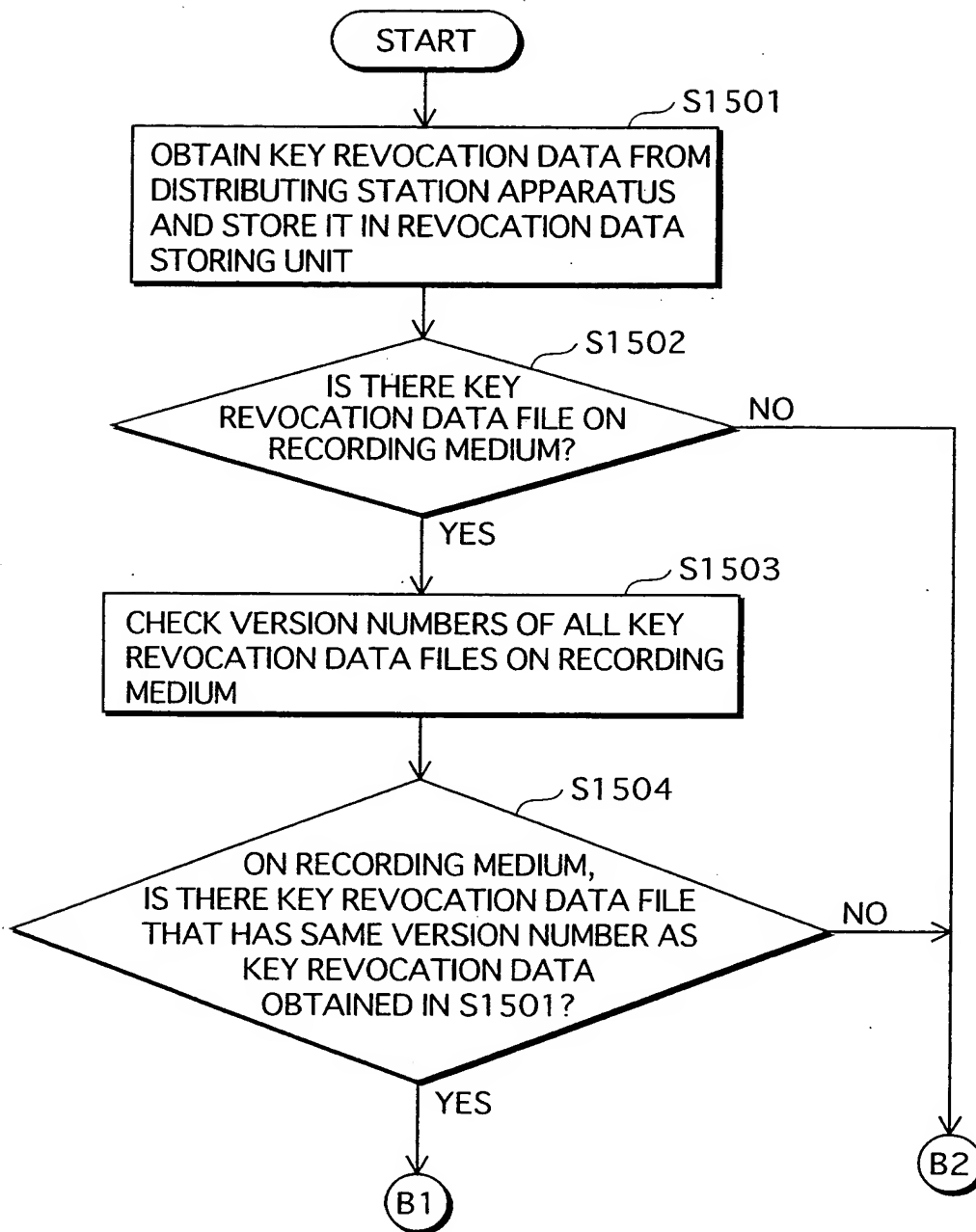


FIG.17

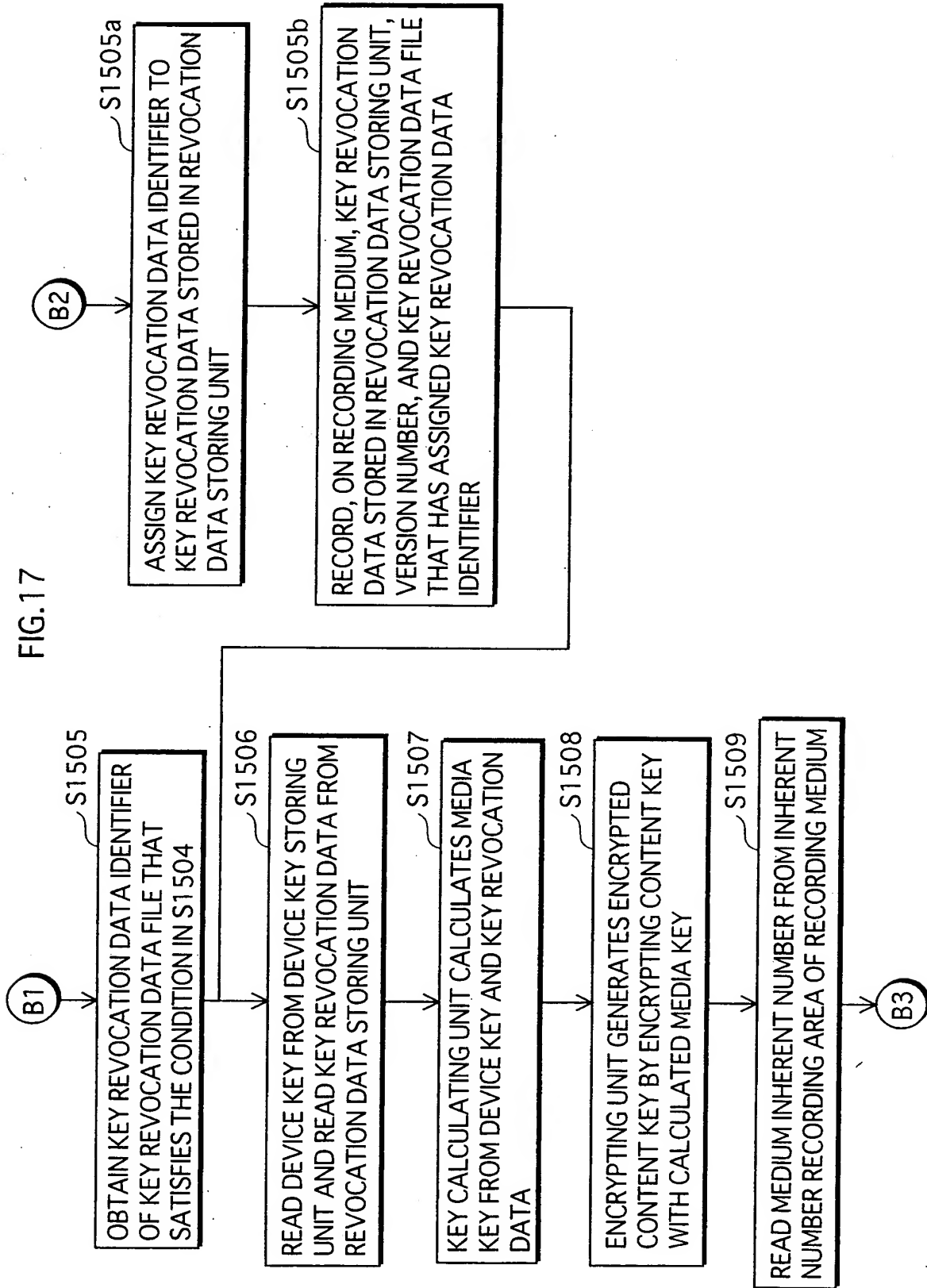


FIG.18

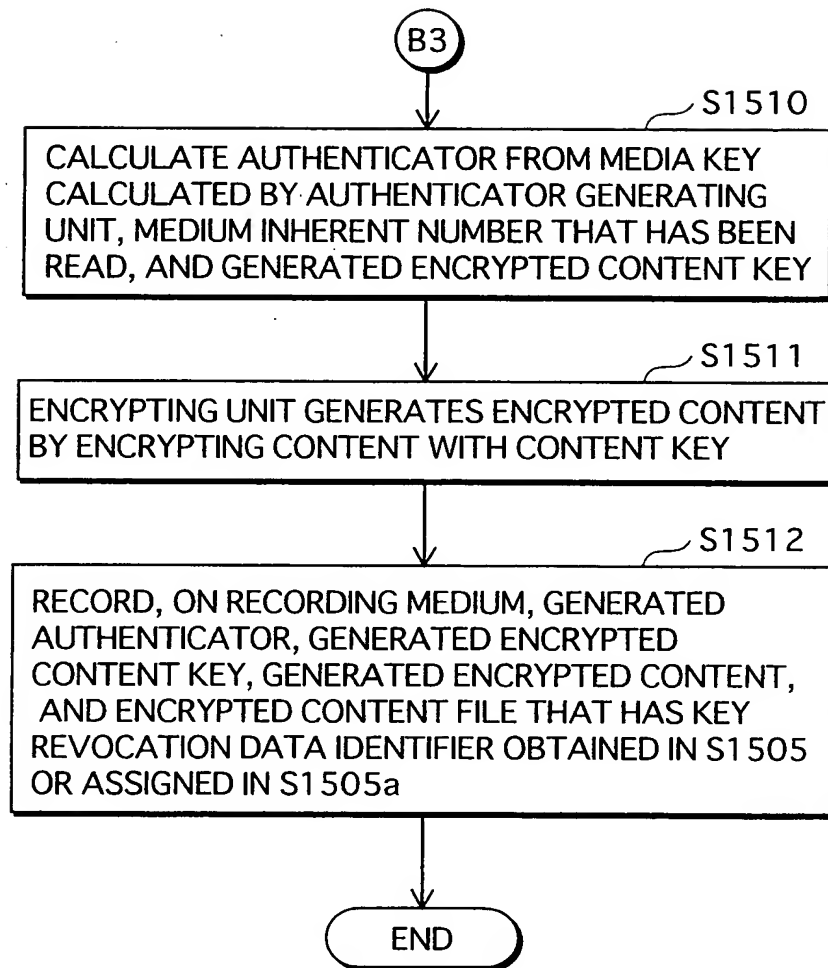


FIG.19

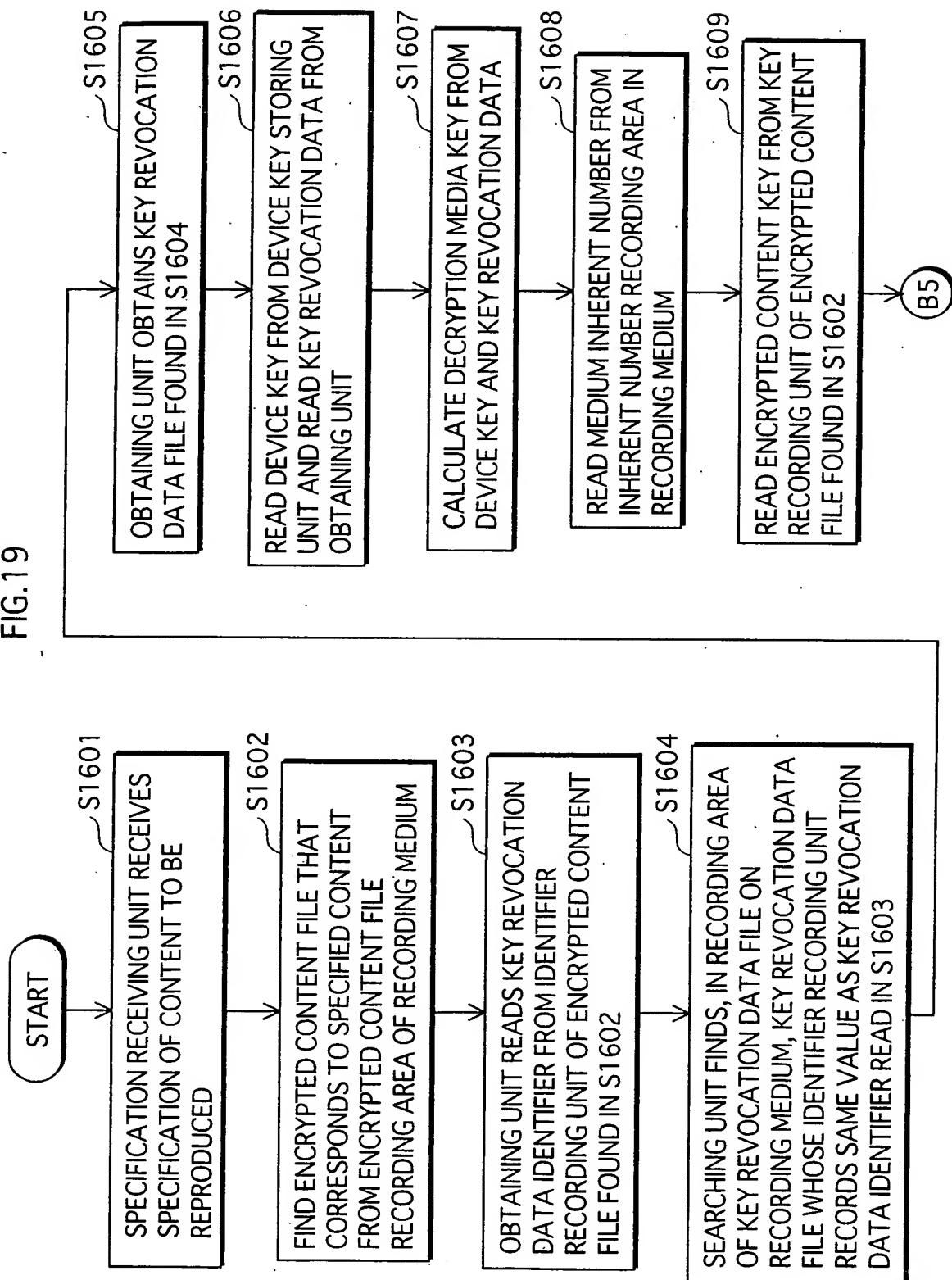


FIG.20

